AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for encrypting data, the method comprising:

providing a data processing system for:

generating a session key;

encrypting the data utilizing the session key using a symmetric encryption routine;

encrypting the session key utilizing a user public key using a first asymmetric encryption routine;

encrypting the session key utilizing a master public key using a second asymmetric encryption routine;

generating a data packet including the encrypted data, the encrypted session key utilizing the user public key and the encrypted session key utilizing the master public key;

transmitting the data packet to a destination data processing system;

decrypting the data packet utilizing the session key using the symmetric encryption routine;

decrypting the session key utilizing a user private key using the first asymmetric encryption routine; and

decrypting the encrypted session key utilizing a master private key using the second asymmetric encryption routine.

2. (Cancelled).

3. (Cancelled).

4. (Cancelled).

5. (Cancelled).

6. (Cancelled).

7. (Previously Presented) The method, as set forth in claim 1, further comprising storing a user's private key on a data storage medium coupled to the destination data processing system.

8. (Previously Presented) The method, as set forth in claim 1, further comprising storing the master private key on a data storage medium coupled to the destination data processing system.

9. (Previously Presented) The method, as set forth in claim 7, further comprising retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

10. (Previously Presented) The method, as set forth in claim 1, further comprising retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

11. (Original) The method, as set forth in claim 1, further comprising utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

12. (Currently Amended) A public key data encryption system wherein each user has a private key and a certificate containing data pertaining to the user including the user's public key, the encryption system comprising:
a master public key;

a first data processing system operable to generate a session key, to encrypt data using the session key using a symmetric encryption routine, to encrypt the session key with the user's public key using a first asymmetric encryption routine, to encrypt the session key with the master public key using a second asymmetric encryption routine, to generate a data packet including the encrypted session keys and the encrypted data, and to transmit the data packet to a second data processing system;

the second data processing system operable to:

decrypt the data packet utilizing the session key using the symmetric encryption routine;

decrypt the session key utilizing a user private key using the first asymmetric encryption routine; and

decrypt the encrypted session key utilizing a master private key using the second asymmetric encryption routine.

13. (Cancelled).

14. (Cancelled).

15. (Cancelled).

16. (Cancelled).

17. (Cancelled).

18. (Previously Presented) The public key data encryption system, as set forth in claim 12, wherein the user's private key is stored on a data storage medium coupled to the second data processing system.

19. (Previously Presented) The public key data encryption system, as set forth in claim 12, wherein the master private key is stored on a data storage medium coupled to the second data processing system.

20. (Previously Presented) The public key data encryption system, as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the user's private key from a smart card.

21. (Previously Presented) The public key data encryption system, as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the master private key from a smart card.

22. (Previously Presented) The public key data encryption system, as set forth in claim 12, further comprising:
a plurality of master private keys; and
a plurality of master public keys.

23. (Currently Amended) An article of manufacture comprising:
a computer usable medium having computer readable program code embodied therein for encrypting and decrypting data wherein each user has a private key and a public key, the article of manufacture comprising:
a master public key;
a first data processing module operable to generate a session key, to encrypt data using the session key using a symmetric encryption routine, to encrypt the session key with the user's public key using a first asymmetric encryption routine, to encrypt the session key with the master public key using a second asymmetric encryption

routine, to generate a data packet including the encrypted session keys and the encrypted data, and to transmit the data packet to a second data processing module;

the second data processing module operable to:

decrypt the data packet utilizing the session key using the symmetric encryption routine;

decrypt the session key utilizing a user private key using the first asymmetric encryption routine; and

decrypt the encrypted session key utilizing a master private key using the second asymmetric encryption routine.

24. (Cancelled).

25. (Cancelled).

26. (Cancelled).

27. (Cancelled).

28. (Cancelled).

29. (Previously Presented) The article of manufacture, as set forth in claim 23, further comprising:

a plurality of master private keys; and

a plurality of master public keys.